信学技報Vol. 92 No. 355

電子情報通信学会技術研究報告

ISEC92－57～63

〔情報セキュリティ〕

1992年12月7日

社団法人 電子情報通信学会

Mth ＝Γ(ξk)
と定義する。

本稿で提案した所有のモデルでは、切断するべき間接的経路の出口或いは入口のスキーマが所有されている場合が起こりうる。仮にこのスキーマのREAD,WRTEを削除すると、ユーザ各自が作って所有したいスキーマが削除されてしまう事になり、使い勝手が悪くなる怖れがある。この様な場合は例えば
1＝priority(所有スキーマ, Pr'(Oj,Ss,Sd))
1＝priority(所有スキーマ, Pt'(Oj,Ss,Sd))
2＝priority(¬(所有スキーマ), Pr'(Oj,Ss,Sd))
2＝priority(¬(所有スキーマ), Pt'(Oj,Ss,Sd))
フィルタ＝Γ(1)
RW削除＝Γ(2)
とすれば所有スキーマの削除がなく自分自身で作ったスキーマの所有が保証される修正ができる。この様に、関係priorityとΓをアプリケーションごとに適宜設定する事によって、適切な修正が可能となる。

6. むすび

本稿では機密性・完全性を一つのモデルの中で矛盾なく表現し、かつ可用性の高い新しいタイプのセキュリティ・モデルとその評価方法を提案した。まずセキュリティ・モデルの構造を情報のREAD,WRITEを引き起こす要因を表現する層「ユーザ・情報の関係層」と、セキュリティ評価した結果の「アクセス行列層」で定義し、BLPや任意アクセスモデルを表現できる事を示した。「ユーザ・情報の関係層」を適宜設定する事によってセキュリティの性質を表現し、かつ可用性の高いモデルを表現する事が可能である。提案モデルでは「ユーザ・情報の関係層」で情報の所有と情報の伝播順序の指定の概念を導入した。セキュリティ方針は[1]「所有情報について機密性と完全性を保証する」、[2]「単に情報の伝播経路を指定するだけではなく指定された順番通りに情報伝播する事」とした。この様に表現したセキュリティを検証するために、検証方法の必要十分条件を証明し、セキュリティ検証の手法を示した。更に、検証した結果、セキュリティの方針が満たされない場合はセキュリティを満たす様に経路を修正する一般的な手法を示した。
本モデルでは時間的にアクセスの指定が変動するアクセス行列の表現と評価方法については述べていない。また、伝播の順番が決まっている複数の経路間の同期の問題についても触れていない。今後はこの様な動的なモデルを表現・評価する必要がある。その際、本稿で述べた静的なモデルはその核となる。

文献

(1)森住、永瀬、竹中、山下、：”セキュリティの形式評価のための構造記述”、WITA'90, WCIS90'、(1990)
(2) Tetsuya Morizumi, Hiroshi Nagase, Toyofumi Takenaka, Kouichi Yamashita
: An Evaluation of Security Requirements Based on the Capability Model,IEICE TRANSACTIONS, VOL.E 74, NO.8, AUGUST, pp.2160-2165 (1991)
(3)森住哲也、永瀬　宏、竹中豊文：階層的所有権に基づいたセキュリティ・モデル、情報セキュリティ研究会、ISEC90-27 (1990)
(4) D.E.BELL, L.J. LAPADULA : "Secure Computer System: Unified Exposition and Multics Interpretation", Mitre Corp., (1976)
(5)児玉、須田：”システム制御のためのマトリクス理論”、計測自動制御学会

社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.
ISEC92-59(1992-12)

圧縮画像に適したディジタルスクランブルの一方式

勝田　昇　　茨木　晋　　中村　誠司　　村上　弘規

松下電器産業（株）　映像研究所

５４０　大阪府大阪市中央区城見２丁目１番６１号
ツイン２１ナショナルタワー８階

あらまし　ディジタル有料放送に適したスクランブル方式を提案する。放送のディジタル化に伴う、スクランブルにおける課題は、特に効果制御の実現にある。本方式の特徴は、ＭＰＥＧ標準に準拠し圧縮符号化された画像データ中の特定パラメータに対し、その符号化方式に応じて、符号長を変えることなく乱数化することであり、符号化効率を低下させることなく、内容がある程度わかるレベルから秘匿度が十分なレベルまで、スクランブルの効果が制御できることである。本稿では、提案方式の基本仕様を具体的に説明し、画像シミュレーション結果と安全性の検討結果等により、スクランブルに必要な要件を満たした本方式の有効性を示す。

和文キーワード　スクランブル　効果制御　ＭＰＥＧ　符号化パラメータ　安全性　ディジタル有料放送

A New Digital Scrambling Method for Compressed Video Signals

Noboru Katta　　Susumu Ibaraki
Seiji Nakamura　　Hiroki Murakami

Image Technology Research Laboratory
Matsushita Electric Industial Co., Ltd.

8th Floor, TWIN21 National Tower
2-1-61, Shiromi, Chuo-Ku, Osaka, 540, Japan

Abstract

We propose a new digital scrambling method for digital pay TV. A typical scrambling problem of digital TV is the control of the concealed level. By use of this method, we randomize, for each coding methods, the codes of specific parameters in video codes compressed by MPEG, so that without sacrificing compression efficiency, we can conceal the video at several levels ranging from barely visible to nonvisible. The results of simulation and discussion of the security show that this method has the necessary requirement for pay TV.

英文 key words　scrambling, control the concealed level, MPEG, coding parameter, security, digital pay TV

Mth ＝Γ(ξk)
と定義する。

本稿で提案した所有のモデルでは、切断するべき間接的経路の出口或いは入口のスキーマが所有されている場合が起こりうる。仮にこのスキーマのREAD,WRTEを削除すると、ユーザ各自が作って所有したいスキーマが削除されてしまう事になり、使い勝手が悪くなる怖れがある。この様な場合は例えば
1＝priority(所有スキーマ, Pr'(Oj,Ss,Sd))
1＝priority(所有スキーマ, Pt'(Oj,Ss,Sd))
2＝priority(¬(所有スキーマ), Pr'(Oj,Ss,Sd))
2＝priority(¬(所有スキーマ), Pt'(Oj,Ss,Sd))
フィルタ＝Γ(1)
RW削除＝Γ(2)
とすれば所有スキーマの削除がなく自分自身で作ったスキーマの所有が保証される修正ができる。この様に、関係priorityとΓをアプリケーションごとに適宜設定する事によって、適切な修正が可能となる。

6. むすび

本稿では機密性・完全性を一つのモデルの中で矛盾なく表現し、かつ可用性の高い新しいタイプのセキュリティ・モデルとその評価方法を提案した。まずセキュリティ・モデルの構造を情報のREAD,WRITEを引き起こす要因を表現する層「ユーザ・情報の関係層」と、セキュリティ評価した結果の「アクセス行列層」で定義し、BLPや任意アクセスモデルを表現できる事を示した。「ユーザ・情報の関係層」を適宜設定する事によってセキュリティの性質を表現し、かつ可用性の高いモデルを表現する事が可能である。提案モデルでは「ユーザ・情報の関係層」で情報の所有と情報の伝播順序の指定の概念を導入した。セキュリティ方針は[1]「所有情報について機密性と完全性を保証する」、[2]「単に情報の伝播経路を指定するだけではなく指定された順番通りに情報伝播する事」とした。この様に表現したセキュリティを検証するために、検証方法の必要十分条件を証明し、セキュリティ検証の手法を示した。更に、検証した結果、セキュリティの方針が満たされない場合はセキュリティを満たす様に経路を修正する一般的な手法を示した。

本モデルでは時間的にアクセスの指定が変動するアクセス行列の表現と評価方法については述べていない。また、伝播の順番が決まっている複数の経路間の同期の問題についても触れていない。今後はこの様な動的なモデルを表現・評価する必要がある。その際、本稿で述べた静的なモデルはその核となる。

文献

(1)森住、永瀬、竹中、山下、：”セキュリティの形式評価のための構造記述”、WITA'90, WCIS90'、(1990)
(2) Tetsuya Morizumi, Hiroshi Nagase, Toyofumi Takenaka, Kouichi Yamashita
: An Evaluation of Security Requirements Based on the Capability Model,IEICE TRANSACTIONS, VOL.E 74, NO.8, AUGUST, pp.2160-2165 (1991)
(3)森住哲也、永瀬　宏、竹中豊文：階層的所有権に基づいたセキュリティ・モデル、情報セキュリティ研究会、ISEC90-27 (1990)
(4) D.E.BELL, L.J. LAPADULA : "Secure Computer System: Unified Exposition and Multics Interpretation", Mitre Corp., (1976)
(5)児玉、須田：”システム制御のためのマトリクス理論”、計測自動制御学会

社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.
ISEC92-59(1992-12)

圧縮画像に適したディジタルスクランブルの一方式

勝田　昇　　茨木　晋　　中村　誠司　　村上　弘規

松下電器産業（株）　映像研究所

５４０　大阪府大阪市中央区城見２丁目１番６１号
ツイン２１ナショナルタワー８階

あらまし　ディジタル有料放送に適したスクランブル方式を提案する。放送のディジタル化に伴う、スクランブルにおける課題は、特に効果制御の実現にある。本方式の特徴は、ＭＰＥＧ標準に準拠し圧縮符号化された画像データ中の特定パラメータに対し、その符号化方式に応じて、符号長を変えることなく乱数化することであり、符号化効率を低下させることなく、内容がある程度わかるレベルから秘匿度が十分なレベルまで、スクランブルの効果が制御できることである。本稿では、提案方式の基本仕様を具体的に説明し、画像シミュレーション結果と安全性の検討結果等により、スクランブルに必要な要件を満たした本方式の有効性を示す。

和文キーワード　スクランブル　効果制御　ＭＰＥＧ　符号化パラメータ　安全性　ディジタル有料放送

A New Digital Scrambling Method for Compressed Video Signals

Noboru Katta　　Susumu Ibaraki
Seiji Nakamura　　Hiroki Murakami

Image Technology Research Laboratory
Matsushita Electric Industial Co., Ltd.

8th Floor, TWIN21 National Tower
2-1-61, Shiromi, Chuo-Ku, Osaka, 540, Japan

Abstract

We propose a new digital scrambling method for digital pay TV. A typical scrambling problem of digital TV is the control of the concealed level. By use of this method, we randomize, for each coding methods, the codes of specific parameters in video codes compressed by MPEG, so that without sacrificing compression efficiency, we can conceal the video at several levels ranging from barely visible to nonvisible. The results of simulation and discussion of the security show that this method has the necessary requirement for pay TV.

英文 key words　scrambling, control the concealed level, MPEG, coding parameter, security, digital pay TV

1. まえがき

近年、ディジタル画像符号化技術の進展に伴い映像信号のディジタル伝送が実用化されつつある。放送分野においても、衛星のトランスポンダー一本で複数の動画が同時に送れることや、伝送時に画質の劣化が少ないことなどの特徴が注目されており、特に米国では、地上波のＨＤＴＶ放送方式の有力な候補の多くがディジタル方式を採用している[1]。

一方、放送衛星や通信衛星の利用に伴い、テレビ放送も多チャンネル化し、これらのチャンネルの多くは、有料放送を行う方向にある。日本でもＪＳＢのＷＯＷＯＷチャンネルに代表される有料放送が行われており、ディジタル放送開始時において有料放送技術は、不可欠なものであると考えられる。

本稿では、有力な圧縮方式であるＭＰＥＧ標準[2][3]に準拠した画像データ中の、特定パラメータに着目し、それらを示す符号語をその符号長を変えることなく乱数化することを特徴とするスクランブル方式を提案する。まず、第２章では、有料放送への要件のうち、特に放送のディジタル化に伴う課題を示す。第３章では、圧縮符号化を含む伝送系でのスクランブルする位置の問題を検討する。第４章では、ＭＰＥＧ標準について簡単に説明する。そして、第５章で提案方式について説明し、第６章では、本方式の安全性等を検証し、その有効性を示す。

2. ディジタル放送におけるスクランブルの課題

有料放送におけるスクランブルに対する要件としては以下の３つが上げられる。

(1)安全性
(2)効果制御
(3)回路規模が大きくならない

これらの要件は、不正な視聴を防ぐと共に、スクランブルシステムの導入に伴う、放送局あるいはそのサービスをうける正規加入者の負担を、極力おさえて健全な有料放送の経営を行う上で不可欠なものである。このうち(2)の効果制御は、非加入者に放送サービス自体の存在を知らせることや、加入意欲を高めるといった加入者勧誘効果を持たせる目的で、内容はわかるが視聴し続けるには十分ではない程度に、画像の撹拌量を制御することであり、現在アナログ伝送系でのＪＳＢの有料放送においては常時効果制御状態でスクランブル放送が運用されている。

しかしながら、ディジタル放送では、伝送される画像情報が圧縮符号化されるため、この効果制御を行うことが困難である。圧縮符号化後に単に撹拌量を制御するのでは、再生時に全データが読み取り不能になってしまったり、また、圧縮符号化前に撹拌処理を行うと、圧縮符号化を困難にしてしまうなど、放送のディジタル化に伴う重要な課題であった。

3. スクランブル処理の位置問題

図３－１は、ディジタル伝送時の処理のブロックを示したものである。特徴は、画像が圧縮符号化処理されることであり、スクランブル処理する位置としては、圧縮符号化前と後が考えられる。以下、２つの場合について問題点を検討する。

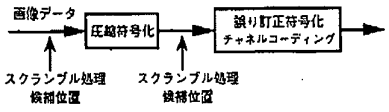

図３－１　ディジタル伝送系の処理ブロック

3. 1　圧縮符号化前スクランブル

圧縮符号化前にスクランブルする場合、スクランブル処理が、圧縮符号化で用いる画像の特徴を維持しており圧縮符号化可能である限り、スクランブル画像がそのまま伝送され、再生されるため、効果制御は容易である。また、必要に応じてデスクランブラーを接続することができるので、再生処理とデスクランブル処理の切り分けができる利便性やコスト面も有利な位置である。しかしながら、テレビの放送を行うレベルの画質を得る符号化では、高能率符号化を実現するため、時間軸と空間軸の両方の画像データの特徴を利用するため、その特徴を維持したままでスクランブル処理し、効果制御を実現することは困難である。さらに、特徴を崩すスクランブル処理は、エントロピーが増加し、圧縮効率が低下するので、その同じビットレートで伝送できる再生画像の劣化を引き起こしてしまう。

3. 2　圧縮符号化後のスクランブル

圧縮符号化後にスクランブルする場合、再生側で通常の再生処理中に、デスクランブル処理が挿入されることになり、利便性ではやや劣る。しかし、スクランブルするデータが、すでに伝送に適応したビットレートに符号化されたビット列であるため、ビット長さえ増えなければ、完全に乱数化しても伝送系には問題を生じない。そのため、安全性の高いスクランブルが容易に行うことができる。

しかしながら、圧縮符号化されたデータが、可変長符号を含む場合は、効果制御を行うことが困難である。図３－２に可変長符号を含むスクランブルデータの再生例を示す。再生器では、１ビット反転されたデータであっても、そのデータを異なった符号長のデータと解釈したり、コードブック内に存在しないデータと解釈することにより、それ以降のデータが全く解読できず、再生不能になる。さらに、再生側のリカバー処理の仕方によっては、再生されるスクランブル画像が異なってくることも考えられ、単にランダムにビット反転するような乱数化では、効果制御を実現することはできない。

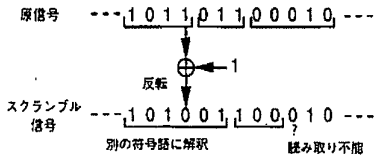

図３－２　１ビットの反転で再生不能になる例

4. ＭＰＥＧ標準

ＭＰＥＧ標準における符号化は、画像の時間軸相関を利用した動き補償フレーム間予測と空間軸相関を利用したＤＣＴ変換符号化によるデータを可変長符号化する方式である。

図４－１は、動き補償フレーム間予測による符号化処理の説明図である。画像中の各フレームは、その符号化の仕方によって３つのフレームがある。１つは、フレーム内だけでＤＣＴ符号化するＩフレームであり、２つめは、過去のフレームからの予測値をもとにその予測差信号のみをＤＣＴ符号化するＰフレーム、そして、３つめは、過去と未来のフレームの両側のフレームから予測画像を生成し、それとの予測差信号のみをＤＣＴ符号化するＢフレームである。これらのフレームをアプリケーションの特徴に応じて最も符号化しやすいように配置すればよく、図に示したのは、代表的なフレームの配置と予測順である。さらに、図４－２に全体的な処理のブロック図を示す。次に、符号化されたデータの構造について説明する。図４－３に示すように、４つの層で構成され、各層はそれぞれ３２ビットの開始コードを含むヘッダ部と、その後に１つ以上の下位層を含む。一番上のシーケンス層は、１つの動画像のシーケンスで番組等を表す。グループオブピクチャー（以後ＧＯＰ）層は、任意の長さのフレームで構成される。ピクチャー層は、１フレームに相当する。スライス層に含まれるマクロブロック層は、画像中１６×１６画素領域の層であり、８×８の画素を１ブロックとして、輝度４ブロック、色差２ブロックからなる。動き補償フレーム間の予測処理は、このマクロブロック単位で行い、ＤＣＴは、８×８画素のブロックで行なう。従って、マクロブロック中には、動きベクトル、ＤＣＴ係数の直流および交流成分等の符号化データが含まれる。そして、これらは、可変長符号と固定長符号とに符号化されビット列を形成している。

以上のように、ＭＰＥＧ標準の符号化の特徴は、

(1)画像の空間軸相関および時間軸相関を利用した高能率符号化であること
(2)符号化されたビット列は、可変長符号と固定長符号で構成されていること

である。

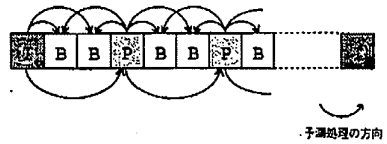

図４－１　ＭＰＥＧ標準のフレーム間予測処理

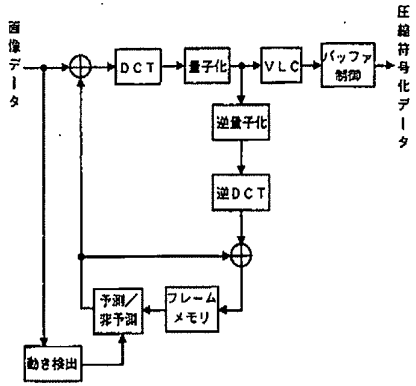

図４－２　ＭＰＥＧ標準の符号化処理

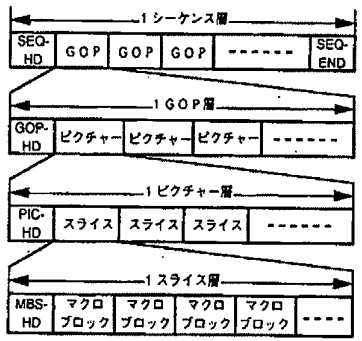

図４－３　ＭＰＥＧ標準でのデータ構造

５．　提案方式

５．１　基本方式

本章では、ＭＰＥＧ標準に適したスクランブル方式を具体的に説明する。

ＭＰＥＧ標準に準じた信号の特徴は前章で示したとおりであり、まず、スクランブルの位置は、圧縮効率に影響を与えないために、圧縮符号化後とする。

次に、スクランブル方式であるが、本方式の特徴は、圧縮符号化されたデータに対して、特定パラメータの符号化方式に応じた乱数化を行うことにより、効果制御を実現したことである。

５．２　乱数化するパラメータ

以下の４つのパラメータを乱数化する。

・量子化スケール（固定長符号）
・動きベクトル（可変長符号）
・ＤＣＴ交流成分（可変長符号）
・ＤＣＴ直流成分（固定長符号）

５．３　乱数化処理の内容

符号化の方式により以下の処理を行う

(1)固定長符号

乱数化する固定長符号は、不規則に出現し、各符号のビット長も短いため、ブロック暗号は不適切である。従って、図５－１のように、対象となる符号を検出し、その符号の全ビットに乱数を付加する。

(2)可変長符号

可変長符号は、乱数をランダムに加えるとコードブックにない符号になってしまったり、ビット長の異なる符号として復号される場合があり、スクランブルした符号以外にも大きな影響を与えてしまう。従って、図５－２のように、対象となる符号を検出し、その符号をコードブック内にあるビット長の等しい符号に置き換える。

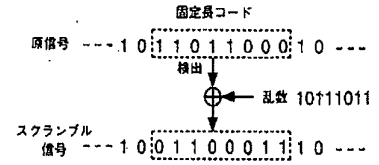

図５－１　固定長符号に対するスクランブル

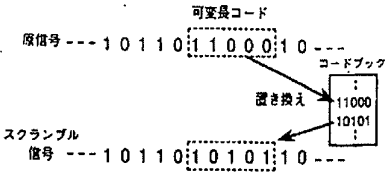

図５－２　可変長符号に対するスクランブル

５．４　量子化スケールスクランブル

【処理】

量子化スケールは、ＤＣＴ係数の交流成分を量子化する量子化幅を示し、ビットレートを目標の値にするために、その値が変更される。各マクロブロック単位のパラメータ（ただし、前マクロブロックと同じ値の場合省略）であり、全５ビットに乱数を付加する。

【効果】

写真１に原画像を、写真２に全ての量子化スケールを乱数化したスクランブル画像を示す。最小マクロブロック単位で、ＡＣ成分のレベルがランダムに変動するので、輝度および色調が変化し、被写体の表面の質感等が失われる効果が得られている。部分的に見ると、マクロブロック間で絵柄が同じ場合、前マクロブロックと同じ量子化スケールが用いられるので、色調は一定である。全体としてうける印象は、十分に視聴に耐えるレベルであり、この方法単独では、効果が不十分である。

５．５　動きベクトルスクランブル

【処理】

動きベクトルは、縦方向と横方向の動きによる前のマクロブロックとの差信号を、図５－４に示すコードブックで符号化したもので、マクロブロック単位のパラメータである。最下位のビットは符号ビットになっており、このビットを反転してもコードブック内の符号となる。そこで、この符号ビットに乱数を付加する。

【効果】

図５－４にスクランブルによる画像への効果を示す。同図(a)は、正常な動き補償予測であるが、スクランブルされることによって同図(b)のように予測フレーム中の誤った所からデータを取り込むことになるため、画像が大きく乱れることになる。ベクトルの方向は、縦横で４通りであり、その内一つが正しい方向なので、残り３通りに誤る。この誤りは、動きベクトルが差信号なので、次のマクロブロックに波及し、さらに、Ｐフレームで発生した誤りは、それから予測されたＰ、Ｂフレームに広がり、次のＩフレームまで影響を与える。写真３は、Ｂフレームでのスクランブル画像である。Ｉフレームには影響がないが、通常大半のフレームがＰまたはＢフレームとなるため視覚的には、影響が大きい。また、部分的には、動きの大きい部分に、より効果が得られている。全体として、物体の動きが非常に不規則で見づらいものとなる。

motion VLC code	little	big
0000 0011 001	-16	16
0000 0011 011	-15	17
0000 0011 101	-14	18
0000 0011 111	-13	19
0000 0100 001	-12	20
0000 0100 011	-11	21
0000 0100 11	-10	22
0000 0100 01	-9	23
0000 0101 11	-8	24
0000 0111	-7	25
0000 1001	-6	26
0000 1011	-5	27
0000 111	-4	28
0001 1	-3	29
0011	-2	30
011	-1	31
1	0	
010	1	-31
0010	2	-30
0001 0	3	-29
0000 110	4	-28
0000 1010	5	-27
0000 1000	6	-26
0000 0110	7	-25
0000 0101 10	8	-24
0000 0101 00	9	-23
0000 0100 10	10	-22
0000 0100 010	11	-21
0000 0100 000	12	-20
0000 0011 110	13	-19
0000 0011 100	14	-18
0000 0011 010	15	-17
0000 0011 000	N/A	N/A

N/A - These table entries are not used and should not be generated by an encoder.

図５－４　動きベクトルのコードブック

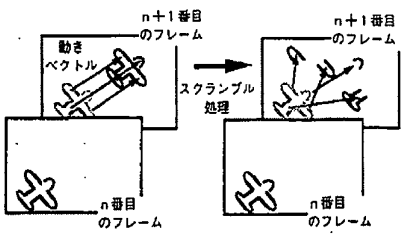

図５－５　動きベクトルスクランブルの効果

5．6　ＤＣＴ係数交流成分スクランブル

【処理】

ＤＣＴの交流成分は、ジギザグスキャンの走査順に、量子化後の値が０であるデータの長さと次に０以外の数値が来たときのレベルの２次元情報により、ハフマン符号化されている。符号化に用いられるコードブックにおいて、最終ビットは符号ビットに割り当てられているので、動きベクトルの場合と同様に、この符号ビットに乱数を付加する。

【効果】

写真４にスクランブル画像を示す。交流成分が劣化するため、解像度が落ちた画像となるが、直流成分が残ることと、ＤＣＴブロックが画像全体の大きさに比べて小さいため、どのような内容の画像であるかは、十分わかるものとなる。特に、細部まで識別できない程度画像から離れた所から見た場合、スクランブルの影響は小さくなる。また、画像の絵柄にも大きく影響し、高域の成分を多く含む細かい絵柄の場合、その効果が大きい。

5．7　ＤＣＴ係数直流成分スクランブル

【処理】

ＤＣＴの直流成分の信号は、マクロブロックが、イントラモードのとき、前のブロックとの差信号として存在する。符号のビット長は、その直前の信号で示され、最大８ビットである。このパラメータもコードブックで符号化されるが、その中に、各ビット長で可能な全てのパターンが存在するので、全ビットに乱数を付加する。

【効果】

写真５に示すように、最も効果が大きい。輝度レベルおよび色相に影響を与えるため、特に大きく劣化した印象を受ける。Ｉフレームをもとに他のフレームは生成されるため、全フレームに効果がある。高域成分は、正しく復号されるため画像中に存在するものは、識別できる。また、直流成分全体に乱数を付加したことになるので、暗号としての強度は最も高い。

5．8　コンビネーションモード

前項までに、４つのパラメーターについてのスクランブルの処理および効果を示したが、その特徴をまとめると、表５－１のようになる。各パラメーターで画像への影響の大きさ、および効果の高いシーン等が異なるため、実際に使用する際には、これらを組み合わせてスクランブル処理することが望ましく、これをコンビネーションモードとする。写真６は、４つの処理を同時に行った場合の画像である。ほぼ画像の内容がわからない程度に撹拌されており、有料放送に必要な秘匿性としては、充分である。また、効果制御については、画像に大きな影響を与えない量子化レベルや、ＤＣＴ係数の交流成分等の組み合せのうち、それぞれのパラメータの特徴が生かされ、より効果的なスクランブルレベルに設定することが可能である。

パラメータ		影響を受けるフレーム	スクランブル効果	
			レベル	特徴
量子化スケール		全フレーム	小	全体的にソフトな効果
動きベクトル		P，Bフレーム	やや大	動きの大きい画像には効果大
DCT係数	交流成分	全フレーム	小	絵柄の細かい画像には効果大
	直流成分	全フレーム	大	輝度、色相ともに効果大

表５－１　各スクランブル方式の特徴

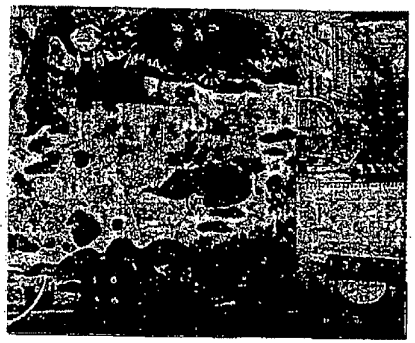

写真１　原画像

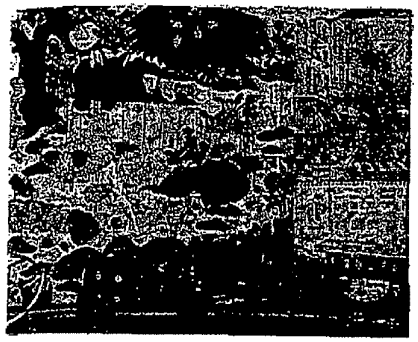

写真２　量子化スケールスクランブル画像

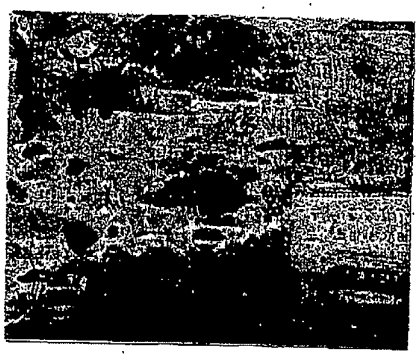

写真３　動きベクトルスクランブル画像

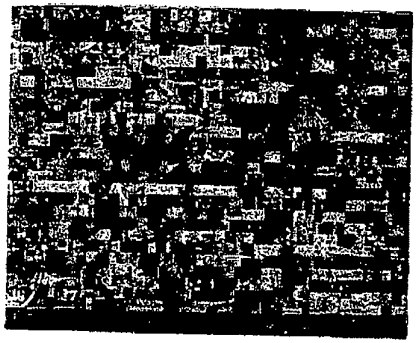

写真４　ＤＣＴ係数交流成分スクランブル画像

写真５　ＤＣＴ係数直流成分スクランブル画像

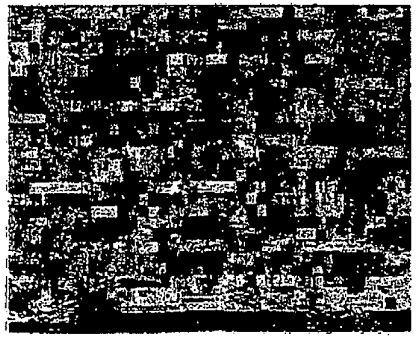

写真６　コンビネーション画像

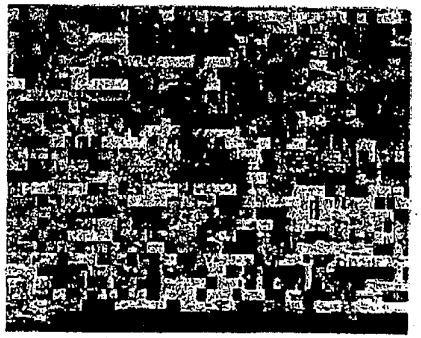

写真７　コンビネーション画像
（１：４乱数使用時）

6. 安全性の検討

6.1 安全性基準

スクランブルデコーダを図6－1の構成として以下の検討を行った。同図において、暗号化されて送られてきたスクランブル鍵およびスクランブルモードは、デスクランブル処理装置で抜取られ、セキュリティ処理装置で復号される。復号されたスクランブル鍵から乱数発生器1で発生した乱数seedsとコンビネーションモードCmは、デスクランブル装置内の乱数発生器2および制御装置にそれぞれ与えられ、乱数発生器2から発生された乱数が、コンビネーションモードで指定される特定パラメータの対象ビットに付加される。すなわち、デスクランブル処理装置には、単に画像データのスクランブル処理機能を持たせ、有料システムの安全性にかかわる機能は、スクランブル鍵の復号処理を行うセキュリティ処理装置に依存させるものとする。

この構成におけるスクランブル方式として必要な安全性基準を、以下の3つに定めた。

（1）鍵パターンが十分とれること。

（2）視聴に十分耐える画質を再生するような正規の鍵以外の鍵が、全鍵数に比べて十分少ないこと。

（3）鍵に関係なくある決まった単純な処理の繰り返し等で解読されないこと。

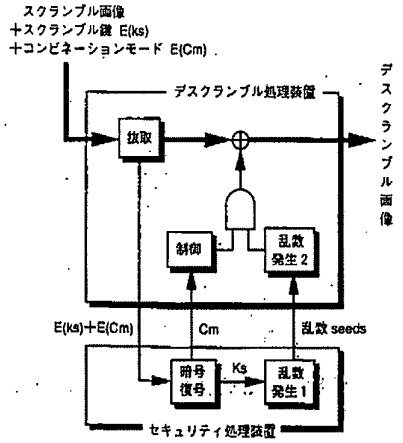

図6－1 スクランブルデコーダの構成

6.2 鍵パターン

本方式において取り得る鍵パターン数は、多くともスクランブルの対象となるビット数である。その数は、画像毎で異なるが、1フレームあたりでは、高々2万ビット弱であり、実際の画像では、Iフレームで3000ビット程度、Pフレームで2000ビット程度、Bフレームで500ビット程度であった。運用上の鍵がスクランブル鍵であり、それから発生される乱数が鍵パターンに相当する。スクランブル対象ビット数が上記の場合、スクランブル鍵として32ビットあるいは、64ビット程度を与えれば、十分な鍵パターン数が得られる。

6.3 有効な鍵数

前節では、十分な鍵パターン数がとれることを示したが、正規のスクランブル鍵以外にも、十分視聴に耐える程度の画像を再生できる乱数を発生する鍵が存在する。本方式は、特定パラメータのみをスクランブル対象ビットとしているので、例えば、Bフレームの約300ビットのスクランブル対象ビットへ付加される乱数が、正しい乱数と数ビットしか異ならない場合、ほとんど問題のない画像が復元されることが予測される。従って、このような乱数を与える鍵が、全体の鍵数に対し高い割合で存在するならば、実質的に有効な鍵数は、その比率によって制限されるし、また、適当にでたらめな鍵を入力することで、ある程度視聴に耐える画像を得るという不正に対する安全性が低くなる。

この問題に対しては、まず、スクランブル対象ビットに付加する段階での乱数を評価する。スクランブル鍵から乱数を発生するアルゴリズム（図6－1における乱数発生1および2）が理想的であれば、異なる鍵から発生される乱数と一致するビット数の確率分布は、二項分布に一致する。従って、乱数が十分長ければ、半分程度のビットは一致するが、極端に多くのビットが一致する割合は小さく問題はない。実用上、乱数発生器は十分理想的なものが用意できるし、乱数も十分長くすることができる。

次に、再生画像を評価する。異なる乱数において均等に80％以上のビットが一致した特別な場合を想定すると、これは、例えば、各スライス層中のスクランブル対象ビットが20ビットであるとした場合、このうち16ビット以上が一致することであり、このことがおこる確率は、0.2％程度である。さらに、1フレーム内で起こる確率は、それの30乗になるし、1秒の動画になるとさらに30乗になり、この様なことが起こり得る確率は、ほとんど0である。写真7は、乱数中の1と0の比率を1：4にした場合のスクランブル画像である。これは、写真6の画像に対するデスクランブルにおいて、前記の特別な場合が発生した時に得られる再生画像に相当すると考えられるが、この場合でさえ、なお十分なスクランブル効果が認められる。従って、仮にかなりのビットが一致してもスクランブル効果は十分得られるといえる。これは、符号化方式が、予測符号化を採用しているため、スクランブルされた効果が、そのまま後の部分にも伝搬するためである。したがって、適当に鍵を入力した程度では、視聴できる程度の画像を得ることはできない。

以上のことから、ほとんどの鍵を有効な鍵として用いることができる。

6.4 鍵を用いない解読

各方式について、画像特有の性質等を用いて解読を試みる場合について考える。

まず、量子化スケールについては、ビットレートを目的の値に近づけるため、変更されるものなので、バッファに残るビット数をシミュレートして、量子化スケールを決定することは、比較的容易である。

動きベクトルについては、動いている物体等を認識し、通常おこりにくい不連続な変化を特徴として検出するなどして、ある程度の復元が可能であろうが、物体の認識等のこれらの処理は、複雑であり現実的でない。

ＤＣＴ交流成分については、既に差信号であることなどから、数ブロックについて連続な絵になるように、とり得るパターンについて調べる以外に特に効率的な方法はなく、これも複雑な処理といえる。

ＤＣＴの直流成分についても、イントラブロックに関して符号語の全ビットに乱数を付加するので、鍵なしの解読は困難である。

以上、解読には、処理の複雑さや困難さから、高速かつ大容量装置等が必要であり、鍵を用いない解読に対する強度は、実用上、十分と考えられる。比較的容易と考えられる量子化スケールに対する解読も、この方式単独では、スクランブル効果が不十分なこともあり、他の方式との組み合わせで運用すれば問題ない。

6.5 スクランブル鍵の更新

スクランブル鍵の更新方法を決定するにあたては、安全性以外の内容も含めて、

（1）不正解読に対する安全性の点で、スクランブル鍵の更新周期はできるだけ短くする。

（2）伝送するスクランブル鍵を極端に多くすることは困難である。

（3）セキュリティ処理装置から供給する乱数は、実用上、画像データの内容に関係なく、規定のデータ単位が望ましい。

ことを考慮して、以下のような運用を考える。

まず、グループオブピクチャー毎に、64ビットのスクランブル鍵を暗号化して伝送する。図6－1のデコーダにおいて、セキュリティ処理装置では、それを復号し、スクランブル鍵をもとにスライス層毎に32ビットの乱数を生成して、デスクランブル処理装置にあたえる。デスクランブル処理装置では、さらにこの32ビットの乱数を種として乱数を発生し、画像データのビットを反転する。

グループオブピクチャーは、約0.5秒程度の短い時間が標準的であり、さらに、ソフトウェアによる暗号処理に十分な時間であることからも、スクランブル鍵更新周期としては適当である。この場合、伝送するスクランブル鍵の量にも問題はない。また、エラー等で再生不能になっても、復帰できる最小単位であるスライス層毎に、セキュリティ処理装置から乱数を供給するため、セキュリティ処理装置での乱数発生アルゴリズムを強固にすれば、その乱数を得ることは困難であり、高い安全性が確保できる。

7. あとがき

本稿では、まず、有料放送におけるスクランブルに対する要件のうち、放送のディジタル化に伴い特に課題となるのが効果制御であることを示した。そこで具体的に、ＭＰＥＧ標準に準拠して高能率符号化された画像データの４つの特定パラメータに着目し、そのビット長を変えることなく、スクランブルすることによって、圧縮効率を維持したままで、内容がある程度わかるレベルから秘匿性が十分なレベルまで効果制御を行えるスクランブル方式を提案し、その実用面での安全性を示した。さらに要件として示した回路規模については、ハード化にあたり、画像の圧縮符号化および復号化処理の過程に、スクランブル処理に対応した機能をもたせれば、スクランブルによる負担も比較的少なく実現できることが予測できることから、本方式は、全ての要件を満足した方式であるといえる。

今後は、本方式をもとに、さらに、ディジタル放送の実用化に向けて最適なスクランブル方式の検討を進める予定である。

参考文献

[1]W.Paik :"Digicipher™ - All Digital, Channel Compatible, HDTV Broadcast System", IEEE Trans. on Broadcasting, Vol. 36, No. 4 (Dec. 1990).

[2]ISO/IEC JTC1/SC2/WG11:"MPEG Video Simulation Model Three (SM3)", MPEG90/041 (July 1990).

[3]DRAFT INTERNATIONAL STANDARD ISO/IEC DIS 11172:"Information Technology - Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5Mbits/s", (1992).

社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.
ISEC 92-60 (1992-12)

IDによる共通暗号化鍵生成方式
— 逐次加算形 乱数項消去法の提案 —
（第３報，田中の指摘に応えて）

† 辻井 重男　‡ 荒木 純道　†† 趙 晋輝
‡‡ 田中 初一　‡ 関根 孝司　† 松崎 義寛

† 東京工業大学 電気電子工学科　‡ 埼玉大学 電気電子工学科
†† 中央大学 電気電子工学科　‡‡ 神戸大学 電気電子工学科

† 152 東京都 目黒区 大岡山 2-12-1

あらまし

本稿では、共通鍵生成の階層について簡単に述べ、べき積を用いたID情報に基づく鍵共有方式が線形代数的な結託攻撃に耐えるための条件を明らかにする。そして、この条件を満たすような鍵共有方式の一例を示す。

和文キーワード　鍵共有方式　離散対数問題　結託攻撃　情報セキュリティ　暗号理論

A Simple ID-based Scheme for Key Sharing
— 3rd version, reply to Tanaka's comment —

† Shigeo TSUJII　‡ Kiyomichi ARAKI　†† Jinhui CHAO
‡‡ Hatsukazu TANAKA　‡ Takashi SEKINE　† Yoshihiro MATSUZAKI

† Dept. of Electrical and Electronic Engineering
Tokyo Institute of Technology
‡ Dept. of Electrical and Electronic Engineering
Saitama University
†† Dept. of Electrical and Electronic Engineering
Chuo University
‡‡ Dept. of Electrical Engineering
Kobe University

† 2-12-1 O-okayama, Meguro-ku, Tokyo 152, Japan

Abstract

A hierarchy in a common key generation process is proposed and it is clarified a condition that an ID-based key sharing scheme can resist against linear algebraic conspiracy attack. After that, a new key sharing scheme is proposed.

英文 key words key sharing system, discrete logarithm problem, conspiracy attack, linear algebra attack, ID-based scheme